UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/628,692	07/28/2000	W. Olin Sibert	7451.0025-00	3388

22852 7590 08/09/2006

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/628,692	SIBERT, W. OLIN	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *7-13 and 28-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *7-13 and 28-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *5/30/2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 5/30/2006, applicant amends claims 7, 28, 35, and 42. The following claims 7-13 and 28-47 are presented for examination.

2. The amendments to the specification and the drawings, filed on 5/30/2006 have been considered, and the objection to the specification has been withdrawn in view of the amended specification.

2.1 Applicant's arguments, pages 11-14, filed on 5/30/2006, with respect to the rejection of claims 1-26 have been fully considered, but they are not persuasive. With respect to claim 7, Applicant mentions that Shavit does not disclose a portion of the application's actual code. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., a predetermined portion of the application that includes some of the application's actual code) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). As explained in the rejection below, Benson discloses a challenge means associated with a protected item of the software (see column 17, lines 30-31), the keyfile meets the recitation of the portion of the application that includes at least some code because once the customer installs the keyfile, the protection mechanism permits the customer to execute the protected software (see column 10, lines 47-52), the keyfile contains at least

activation of services of the protected program (see column 17, lines 5-13). Applicant has amended claim 7 to delete the new matter from the previous amendment. Therefore, the scope of claim 7 has been changed. With respect to claims 28, 35, and 42, applicant asserts that both Benson and Shavit does disclose hashing portion of the program. Shavit discloses in addition to selecting portion of the program hashing portion of the program code to render the program relatively difficult to replace the functionality provided by the program (see column 16, lines 30-55). Contrarily to applicant's statement, Examiner does not concede that Benson fails to teach that limitation, the independent claims are either anticipated or rendered obvious in view of Benson. The application portions are described in Applicant's specification as any type of components and the credentials as verification information. To expedite the prosecution, Shavit has been used to show prior art of random selection and one or more cryptographic hashes of "actual code" of the application. It remains the examiner's position that claims 7-13 and 28-47 are still rejected for at least the reasons cited above and in the Office Action.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 7, 10-11, and 13 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,047,242 to **Benson**.

As per claim 7, **Benson** discloses a trusted element for use with a computer system including an insecure arrangement for using an application, the trusted element comprising: in one embodiment, **Benson** discloses a server that meets the recitation of trusted element, that may be on a separate address space and the program is executing in a different space on the user machine considered as insecure, both the server and the program are in the same machine (column 16, lines 55-59 and column 14, lines 5-26), in another embodiment, the program may reside on a floppy disk or CD ROM or downloaded from the Internet (see column 16, lines 8-12). **Benson** discloses a trusted element comprises a decryptor that decrypts a credential (key file) associated with the application, for example (see column 12, lines 63-65); a validator that validates at least one digital signature corresponding to the credential, for example (see column 12, line 55 through column 13, line 15); **Benson** discloses a challenge/response means that meets the recitation of a challenge generator that selects, based at least in part on the credential, at least

one predetermined portion of the application, and issues a challenge requesting a response from the insecure arrangement, the response providing a computation of at least one value based on the selected predetermined portion of the application, for example (see column 12, line 55 through column 13, line 52 and column 10, line 47 through column 11, line 38), Benson discloses that the key file may contain information concerning selective activation of services of the protected program such as execution of a Print service, Save-On-Disk service, date a particular service may execute, etc. that meets the recitation of "predetermined portion of the application including some code" and further discloses performing a validation (authentication) on the key file (credential) to determine whether the key file is valid or has been tampered or whether to deny service to the program (see column 17, lines 1-25 and column 10, lines 29-42; column 12, lines 11-15); **Benson** discloses the challenge/response in another embodiment, for example (see column 9, lines 25-45; column 17, line 25 through column 18, line 55; and column 19, lines 15-53); and a response checker that checks the response against the credential, for example (see column 12, line 50 through column 13, line 18 see also column 1, lines 48-62 and column 2, line 48-51).

As per claim 10, **Benson** discloses the limitation of wherein the challenge generator issues the challenge to the application to compute the value (see column 13, lines 1-39).

As per claim 11, **Benson** discloses the limitation of wherein the challenge generator requests the application to compute a cryptographic hash of the selected portion (see column 13, lines 1-39 and column 14, lines 17-39 and column 15, lines 35-40).

As per claim 13, **Benson** discloses the limitation of wherein the challenge generator selects a byte range within the application (see column 9, lines 40-45).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8-9, 12, and 28-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,047,242 to **Benson** in view of US Patent 6,009,543 to **Shavit**.

As per claim 8, **Benson** discloses different embodiments of portion of the application defined by a credential (see column 19, lines 15-22 and column 6, lines 3-18). The advantage of using randomness is also suggested in Benson (column 9, lines 25-45). The keying material and/or verification information disclosed in Benson can be reasonably interpreted as portions defined by the credentials. **Shavit** in an analogous art teaches randomly selecting a

predetermined portion of the application, including some codes, for example (see column 11 lines 49-57 and column 14, lines 39-63, and column 15, lines 55 et seq.); randomly selecting one of the predefined plural portions, for example (see column 11 lines 49-57). **Shavit** further discloses cryptographic hash of the selected portion (column 16,lines 30-55) and challenge/response mechanism to verify tampering (see column 12, lines 19-52). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Benson** to select randomly the predetermined portion from plural predetermined portions as taught by **Shavit** in order to maintain control over those parties able to use the software, for example (see column 12, lines 56-58). One of ordinary skill in the art would have been motivated to do so because by randomly selected portion needed for the user program to function, it would render it relatively difficult to replace the functionality provided in the missing portion without input from the other program in the trusted side (see column 12, lines 30-58), thereby maintaining control over those parties able to use the software as suggested by **Shavit**.

As per claim 9, **Benson** substantially teaches the claimed trusted element of claim 7. **Benson** does not explicitly teach randomly issuing the challenge during execution of the application. However, **Shavit** in an analogous art teaches the limitation of: wherein the challenge generator issues the challenge during execution of the application by the insecure computing arrangement (see column 12, line 53 through column 13, line 4); and wherein the challenge generator selects a virtual path within the application (see column 5, lines 55-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention

was made to modify the method of **Benson** to issue the challenge during execution of the application as taught by **Shavit** in order to maintain control over those parties able to use the software (see column 12, lines 56-58). This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestions provided by **Shavit** so as to maintain control over those parties able to use the software.

As per claim 12, **Benson** substantially teaches the claimed trusted element of claim 7. **Benson** does not explicitly teach selecting a virtual path within the application. However, **Shavit** in an analogous art teaches the limitation of: wherein the challenge generator selects a virtual path within the application (see column 5, lines 55-67). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Benson** to select a virtual path and challenge during execution of the application as taught by **Shavit** in order to maintain control over those parties able to use the software (see column 12, lines 56-58). This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestions provided by **Shavit** so as to maintain control over those parties able to use the software.

As per claim 28, **Benson** substantially discloses a method for permitting an application executing within the insecure execution space to request one or more services from a trusted element executing in the secure execution space the method comprising: issuing a challenge from the trusted element to an application or agent executing in an insecure execution space, the challenge being based at least in part on randomly selected parts of an authenticated credential,

the challenge requesting the application or agent to provide one or more cryptographic hashes of one or more portions of the application, for example (see column 12, line 55 through column 13, line 52 and column 10, line 47 through column 11, line 38); sending, from the application or agent to the trusted element, said one or more cryptographic hashes of one or more portions of the application (see column 13, lines 1-39 and column 14, lines 17-39 and column 15, lines 35-40); comparing, at the trusted element, information provided by the authenticated credential with said one or more cryptographic hashes of one or more portions of the application (see column 13, lines 1-39 and column 14, lines 17-39 and column 15, lines 35-40); denying the application access to said one or more services if the comparison fails (see column 13, lines 35-39 and column 17, lines 5-20). **Benson** discloses a server that meets the recitation of trusted element, that may be on a separate address space and the program is executing in a different space on the user machine considered as insecure, both the server and the program are in the same machine (column 16, lines 55-59 and column 14, lines 5-26), in another embodiment, the program may reside on a floppy disk or CD ROM or downloaded from the Internet (see column 16, lines 8-12). **Benson** discloses a challenge based at least in part on randomly selected parts of an authenticated credential (see column 19, lines 15-22 and column 6, lines 3-18). The advantage of using randomness is also suggested in Benson (column 9, lines 25-45). The keying material and/or verification information disclosed in Benson can be reasonably interpreted as parts of an authenticated credential and portions of the application. **Shavit** in an analogous art teaches randomly selecting a predetermined portion of the application, including some codes, for example (see column 11 lines 49-57 and column 14, lines 39-63, and column 15, lines 55 et

seq.); randomly selecting one of the predefined plural portions, for example (see column 11 lines 49-57). **Shavit** further discloses cryptographic hash of the selected portion (column 16,lines 30-55) and challenge/response mechanism to verify tampering (see column 12, lines 19-52). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Benson** to select randomly the predetermined portion from plural predetermined portions as taught by **Shavit** in order to maintain control over those parties able to use the software, for example (see column 12, lines 56-58). One of ordinary skill in the art would have been motivated to do so because by randomly selected portion needed for the user program to function, it would render it relatively difficult to replace the functionality provided in the missing portion without input from the other program in the trusted side (see column 12, lines 30-58), thereby maintaining control over those parties able to use the software as suggested by **Shavit**.

As per claim 35, claim 35 recites the same limitation as claim 28 except for incorporating the claimed method in a computer readable medium. Therefore, claim 35 is rejected on the same rationale as the rejection of claim 28.

Claim 42 recites an appliance comprising a secure execution space, an insecure execution space a trusted element operable to execute within the secure execution space. **Benson** discloses a server that meets the recitation of trusted element, and suggests that the server program may be on a separate address space and the program is executing in a different space on the user machine considered as insecure, both the server and the program reside in the same machine (column 16,

lines 55-59), in another embodiment, the program may reside on a floppy disk or CD-ROM or downloaded from the Internet (see column 16, lines 8-12). Therefore, claim 42 is rejected on the same rationale as the rejection of claim 28.

As per claims 29, 33, 36, 40, and 46, the combination of **Benson** and **Shavit** discloses repeating the challenges and portions of the application may overlap (see Shavit, column 15, line 55 through column 16, line 55). Therefore, these claims are rejected on the same rationale as the rejection of claims 35 and 42 above.

As per claims 30, 31, 37, 38, and 44, **Benson** discloses the limitation of further including the step of digitally signing the credential and at least in part encrypted (see column 11, lines 22-51).

As per claims 32, 39 and 45, the combination of **Benson** and **Shavit** discloses the claimed appliance and medium of claims 35 and 42 in which the one or more portions of the application include code (see **Benson,** column 17, lines 1-25 and column 10, lines 29-42; column 12, lines 11-15). See **Shavit**, column 12, lines 30-58. Therefore, these claims are rejected on the same rationale as the rejection of claims 35 and 42 above.

As per claims 34, 41, and 47, the combination of **Benson** and **Shavit** discloses one or more portions of the application corresponds to a predetermined byte range or virtual path in the application (see **Benson,** column 9, lines 40-63).

As per claim 43, **Benson** also suggests using smart card and dongle that meets the recitation of protected environment. It would have been obvious to one skilled in the art to implement the license server in a smart card or dongle in order to protect the challenge mechanism of the license server as suggested by **Benson** (column 16, lines 13-17, lines 40-46). It is also very well known in the art that a program operating in a user computer when protected by a validation system is protected with an authentication program or cryptographic processors that reside in a protected environment. It would also have been obvious to one ordinary skill in the art to use a smart card or any other protecting environment as known in the art to protect the second program and the server program of Shavit for protection against attacks as suggested in Benson .

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CC

Carl Colin
Patent Examiner
August 4, 2006

NASSER MOAZZAMI
PRIMARY EXAMINER

8/7/06